ISSN:0975-9646

A Novel Approach Based Image Tracing

K.Satish Babu, Y N Supraja , S.Karunakar Reddy
Dept. of ECE, Aurora's Technological & Research Institute ,Hyderabad

Abstract - Digital watermarking is a process for modifying physical or electronic media to embed a machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Most commonly, digital watermarking is applied to media signals such as images, audio signals, and video signals. However, it may also be applied to other types of media objects, including documents (e.g., through line, word or character shifting), software, multi-dimensional graphics models, and surface textures of objects[1].
There are several algorithms used for watermarking like LSB Watermarking Technique, Spatial Domain & Frequency domain watermarking. In this paper we are using LSB Watermarking technique as it is robust and secure.
In this project, we present a novel watermarking scheme, which allows inserting and reliably detecting multiple watermarks sequentially embedded into a digital image. The proposed method, based on embedding a preprocessed image by text as well as image watermarking, secure under projection attack and robust against distortion due to basic operations such as storage, transmission, and format conversion.

Keywords: Digital watermarking, DCT, Steganography,Image processing

1. INTRODUCTION

Digital watermarking is a process for modifying physical or electronic media to embed a machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Most commonly, digital watermarking is applied to media signals such as images, audio signals, and video signals. However, it may also be applied to other types of media objects, including documents (e.g., through line, word or character shifting), software, multi-dimensional graphics models, and surface textures of objects[2].
Digital watermarking systems typically have two primary components: an encoder that embeds the watermark in a host media signal, and a decoder that detects and reads the embedded watermark from a signal suspected of containing a watermark (a suspect signal). The encoder embeds a watermark by altering the host media signal. The reading component analyzes a suspect signal to detect whether a watermark is present. In applications where the watermark encodes information, the reader extracts this information from the detected watermark.
Several particular watermarking techniques have been developed. The reader is presumed to be familiar with the literature in this field. Particular techniques for embedding and detecting imperceptible watermarks in media signals are detailed in the assignee's co-pending application Ser. No. 09/503,881 and U.S. Pat. No. 6,122,403, which are hereby incorporated by reference.
One particular problem in digital watermarking applications is synchronizing a detector to deal with geometric warping distortion of a watermarked image. A number of techniques have been developed for dealing with geometric distortion in watermarked images. One technique is to make the watermark more robust to geometric distortion by embedding it in attributes of the image that are relatively invariant to geometric distortion. While this improves detection in some cases, it typically does not address all forms of geometric distortion and more complex, non-linear geometric distortion.

2. LITERATURE SURVEY

More recently, different watermarking techniques and strategies have been proposed in order to solve a number of problems, ranging from the detection of content manipulations, to information hiding (steganography), to document usage tracing. In particular, the insertion of multiple watermarks to trace a document during its lifecycle is a very interesting and challenging application. The main objective is to grant the possibility of directly detecting from the document who was the creator, who had access to the data after its creation, how the property of the document is shared among different users, allowing not only the document tracing (crucial for example in the management of images connected to a legal prosecution), but also data usage monitoring (useful in newspaper documents processing).

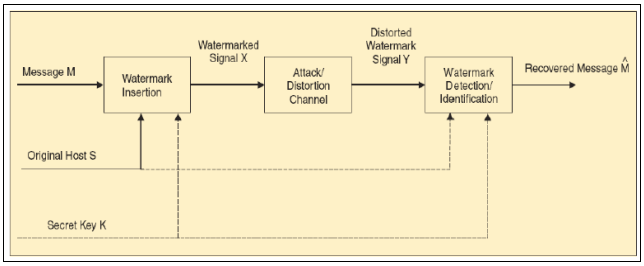
2.1 Security and Medical Information

We have presented here a novel watermarking scheme, which allows inserting and reliably detecting multiple watermarks sequentially embedded into a digital image, as it is required by challenging Digital Right Management applications such as confidential data tracing and shared property handling. The proposed method, based on elementary linear algebra, asymmetric, involving a private key for embedding and a public key for detection. Its robustness against standard image degradation operations (e.g., AWGN addition, JPEG compression, resizing, etc.) has been extensively tested and its security under projection attack has also been proven even though the envisaged applications refers to a collaborative environment, in which malicious attacks are not a critical aspect. Future work will be devoted to the design of a non-collaborative version of the proposed method, addressing non trivial
In order to be effective, a watermark should have the characteristics outlined below.

2.2 Unobtrusiveness

The watermark should be perceptually invisible, or its presence should not interfere with the work being protected. Robustness: The watermark must be difficult (hopefully impossible) to remove. In particular, the watermark should be robust in the following areas: - Common signal

processing: The watermark should still be retrievable even if common signal processing operations are applied to the data.



2.3 Spread Spectrum Watermarking

The watermark should not be placed in perceptually insignificant regions of the image (or its spectrum), since many common signal and geometric processes affect these components. The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum in a fidelity preserving fashion. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise. To solve this problem, the frequency domain of the image or sound at hand is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that the immersed signal must be immune to. We originally conceived our approach by analogy to spread spectrum communications. In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. To insert a watermark in the frequency domain of an image we should first apply DCT(Discrete Cosine Transformation). This is a standard way to represent an image in frequency domain[3].

3. PROPOSED SYSTEM

The proposed method, based on elementary linear algebra, is asymmetric, involving a private key for embedding and a public key for detection. Its robustness against standard image degradation operations has been extensively tested and its security under projection attack has also been proven even though the envisaged application refers to a collaborative environment, in which malicious attacks are not a critical aspect[4]. Here we are providing multiple watermarking concepts, such as the sample image overwrite more than one time on the original image.

4. IMPLEMENTATION & RESULTS

Home screen:

After successful compilation and execution of the project the following screen appears

The home Screen consists of three tabs.

- Image Processing
- Visible watermarking
- Invisible watermarking

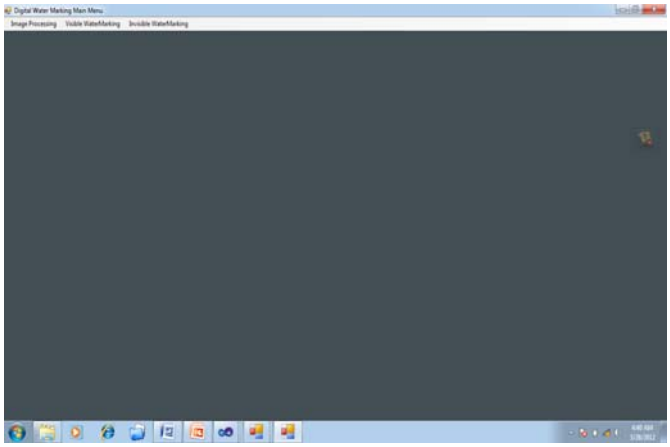
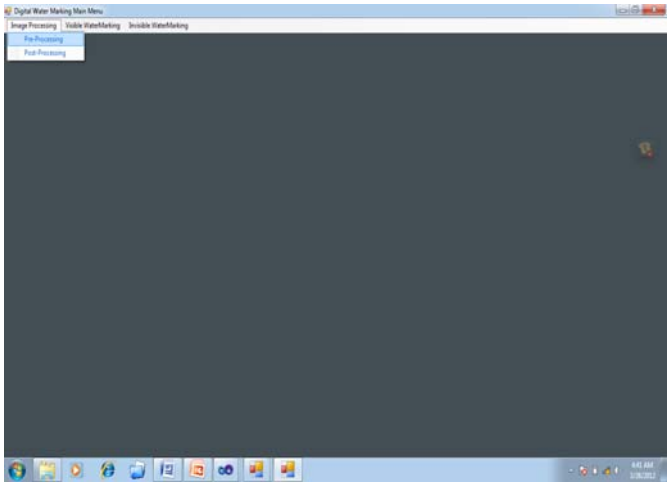


Image processing:

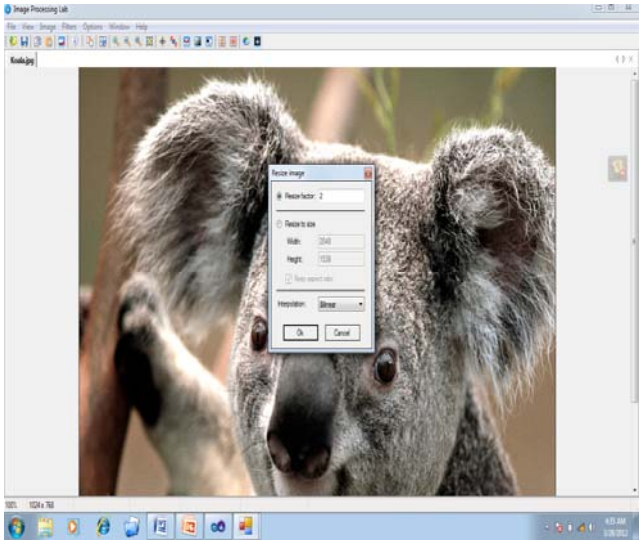
Image processing consists of two options.

- Pre-processing
- Post-processing



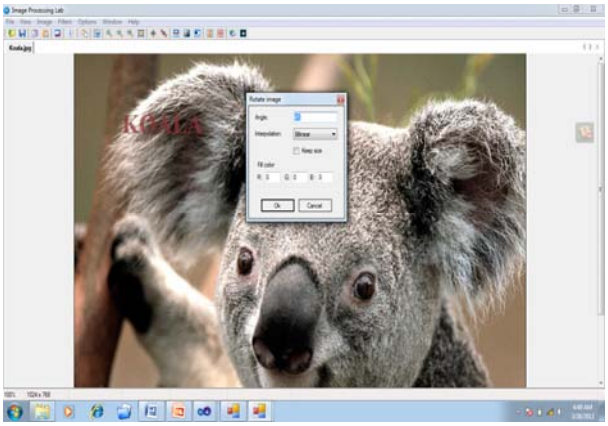
Pre-processing:

In pre-processing we can edit the image before watermarking it. We can resize, zoom, crop etc...



Post-processing:

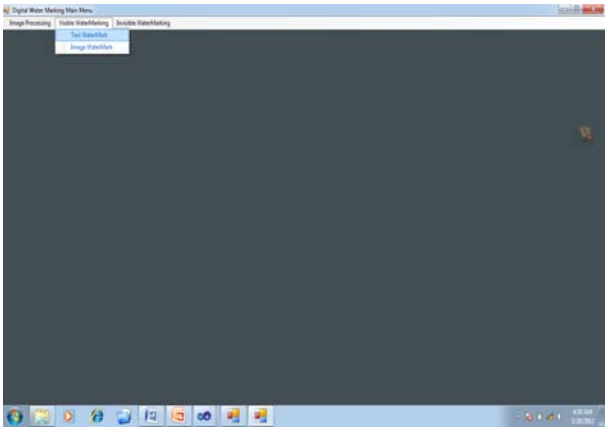
In post-processing we can edit the image after watermarking it. We can resize, zoom, crop etc... the watermarked image.



Visible watermarking:

Visible watermarking consists of two options.

- Text Watermarking
- Image Watermarking



Text Watermarking:

The following figure shows the screenshot of Text watermarking[5] where we have to provide values in the text boxes like enter text to watermark, intensity(alpha),Red, Green, Blue, Font Type and Size, watermark position etc…After providing the information upon clicking the button text watermarking a dialogue box is opened where we have to select an image for watermarking. After selecting the image the Watermarked image appears on the screen.

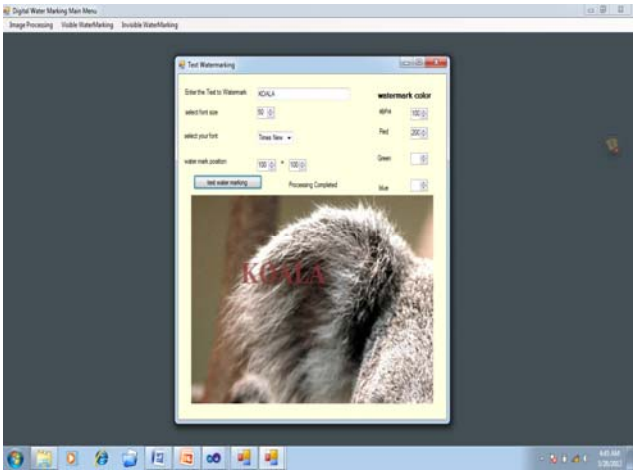
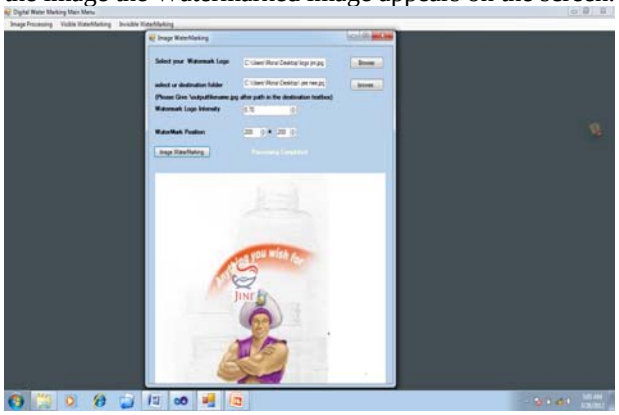


Image Watermarking:

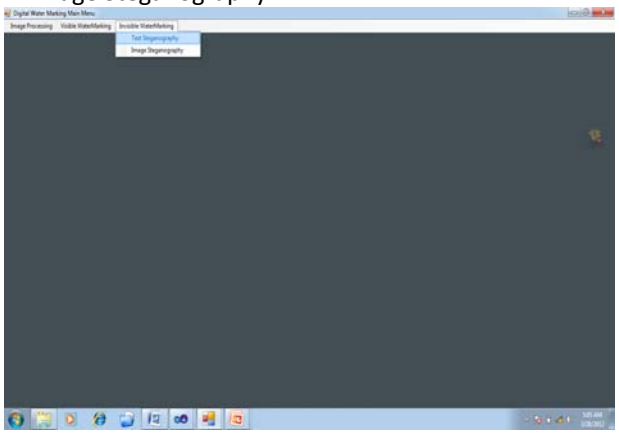
The following figure shows the screenshot of Image watermarking where we have to provide values in the text boxes like watermark logo, intensity, watermark position etc… After providing the information upon clicking the button Image watermarking a dialogue box is opened where we have to select an image for watermarking. After selecting the image the Watermarked image appears on the screen.



Invisible watermarking:

Invisible watermarking consists of two options.

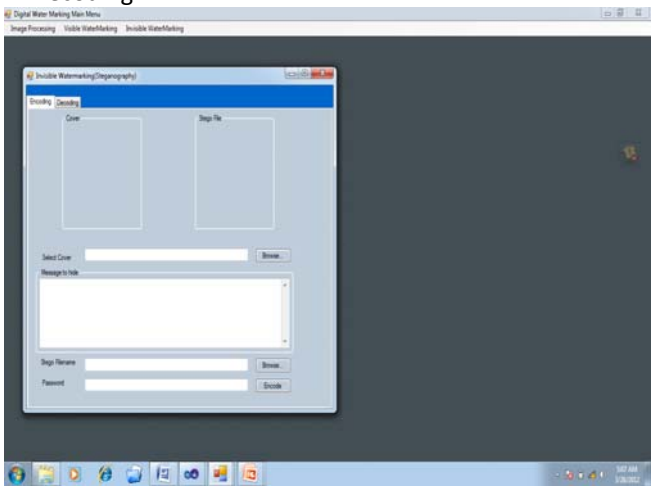
- Text Steganography
- Image Steganography



Text Steganography:

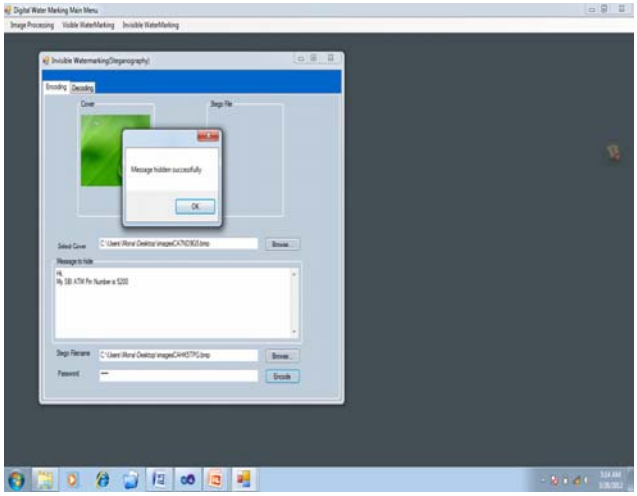
Text steganography consists of two tabs.

- Encoding
- Decoding



Encoding:

In Encoding we need to provide two bitmap images cover image and a stego image.We need to write the message to hide in the space provided and a password is kept. Upon clicking Encode button a message "message hidden successfully" is displayed on the screen.



Decoding:

In Decoding the stego file and password which is used while decoding is to be given. Upon clicking the button Decode the hidden message is displayed.

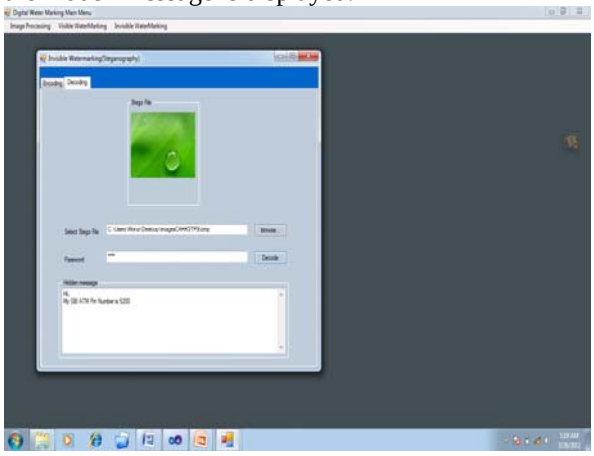
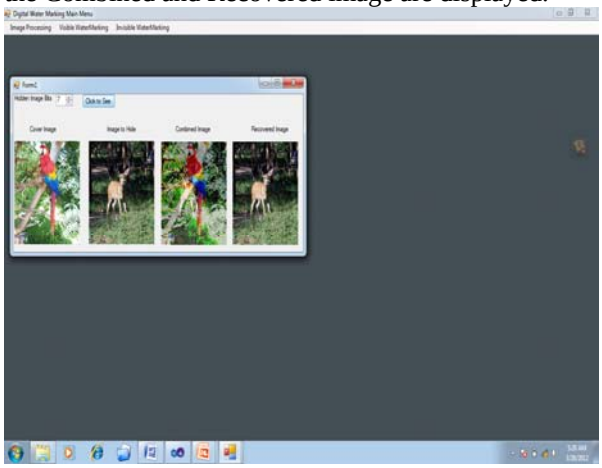


Image Steganography

In Image Steganography number of bits of hidden image that are to be hidden in cover image are given. According to that the Combined and Recovered image are displayed.



5. CONCLUSION

Digital watermarks have been used in the last few years to protect the ownership of digital data. Legitimate business and webmasters have nothing to fear from copyright law or new form of on-line enforcement technology found in digital watermarks and tracking services.

In future Digital watermarking can be applied on audio, video, multimedia etc… Digital Watermarking will steer the future of security over internet

REFERENCES

[1] Kahin B. The strategic environment for protecting multimedia. volume 1, pages 1{8. IMA Intellectual Property Project Proceedings, January 1994.

[2] Comes S. Les traitements perceptifs d'images num_eris_ees. PhD thesis, Universit_e Catholique de Louvain, June 1995.

[3] Olzak L.A. and Thomas J.P. Handbook of perception and human performance vol.1: Seeing spatial patterns. chapter 7.

[3] J.F. Delaigle and C. De Vleeschouwer. Etiquetage d'images num_eriques en vue de la protection des droits d'auteur, Juin 1995.

[4] J.F. Delaigle C. Simon and B. Macq. Talisman (ac019): Technical state of the art. January 1996.

[5] O. Bruyndonckx J.M. Boucqueau and B. Macq. Watermarking: workpackage 5 of accopi. June 1995.

[6] www.google.com

[7] vivekpedia.com

[8] jntuworld.com

AUTHOR'S BIOGRAPHY

Mr K.Satish Babu is currently working as an Associate Professor in the department of Electronics & Communications Engineering, Aurora's Technological & Research Institute Hyderabad. He received his B.E Degree from Osmania University, Hyderabad and M Tech from J N T University . He has over 13 years of teaching experience in the field of Electronics & Communication engineering. His areas of Interests particularly includes VLSI, Digital & Image Processing.

Ms Y. N Supraja is is currently working as an Associate Professor in the department of Electronics & Communications Engineering at Aurora's Technological & Research Institute, Hyderabad. She received her B.Tech Degree from NBKRIST, in the year 2002. and M Tech from KEC in the year 2007 . She has over 10 years of teaching experience in the field of Electronics & Communication engineering. Her ares of interests include digital electronics, VLSI & Image Processing.She has presented many papers in various conferences.

Mr S.Karunakar Reddy is currently working as an Associate Professor in the department of Electronics & Communications Engineering at Aurora's Technological & Research Institute, Hyderabad. He received his B.E Degree and M.Tech from JNTU Ananthapur His research interests include Image & Video processing & Communication systems.